Applicant : Christopher A. Rygaard   Attorney's Docket No.: 18511-008001
Serial No. : 09/851,763
Filed   : May 8, 2001
Page   : 3 of 15

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1.   (Currently amended) A mobile application security system, comprising:

a management and security console computer connected to one or more hosts, each host configured to execute a mobile application that jumps between hosts during execution, the management and security console computer that executes instructions for controlling the security of a mobile application;

one or more host computers connected to the console computer, each host computer executing the mobile application that jumps between the hosts during execution;

the console computer further comprising means for monitoring the security of the mobile application as it jumps between a dispatching host and another host wherein information about the mobile application and the dispatching host is communicated to the management and security console computer[[;]], and wherein the security monitoring means further comprises comprising means for determining if authentication of the dispatching host is required prior to dispatch of the mobile application responsive to determining if the mobile application is a sensitive mobile application and determining if the dispatching node is a vulnerable node, and means for requesting authentication if authentication of the dispatching host is required.

2.   (Cancelled)

3.   (Currently amended) The system of Claim claim 1, wherein the determining requesting means further comprises means for determining if the mobile application being dispatched is a sensitive application and means for requesting requests authentication if a sensitive mobile application is being dispatched.

4.   (Currently amended) The system of ~~Claim~~claim 1, wherein ~~the determining~~ requesting means ~~further comprises means for determining if the dispatching host is vulnerable and means for requesting~~ requests authentication if a mobile application is being dispatched from a vulnerable host.

5.   (Currently amended) The system of ~~Claim~~claim 1, wherein the management and security console computer ~~determining means~~ further comprises means for authenticating the dispatching host based on one or more rules defined by ~~an operator of the system~~ a user.

6.   (Currently amended) The system of ~~Claim 2~~claim 1, wherein the management and security console computer ~~determining means~~ further comprises means for assigning a vulnerable classification or a non-vulnerable classification to each host ~~in the mobile application system~~.

7.   (Currently amended) The system of ~~Claim 2~~claim 1, wherein the management and security console computer ~~determining means~~ further comprises means for assigning a sensitive classification or a non-sensitive classification to each mobile application ~~in the mobile application system~~ as the mobile application is created.

8.   (Currently amended) The system of ~~Claim~~claim 1, wherein each mobile application comprises an itinerary listing a node for each host to which the mobile application jumps in the mobile application system wherein each node indicates if authentication is required to jump from the particular host and wherein ~~the determining~~ requesting means ~~further comprises means for requesting authentication~~ requests authentication based on the node in the itinerary.

9.   (Currently amended) The system of ~~Claim 2~~claim 1, wherein ~~the host~~ a host comprises one or more wireless ~~device~~ devices that are classified as vulnerable.

10.   (Currently amended) A mobile application security method, comprising:
        receiving data about a mobile application at a security node each time the mobile application jumps from a dispatching host to another host ~~in a mobile application system~~; and

Applicant : Christopher A. Rygaard   Attorney's Docket No.: 18511-008001
Serial No. : 09/851,763
Filed   : May 8, 2001
Page   : 5 of 15

determining if authentication of the dispatching host is required prior to dispatch of the mobile application, including determining if the mobile application is a sensitive mobile application and determining if the dispatching node is a vulnerable node; and

requesting authentication if authentication of the dispatching node is required.

11.   (Cancelled)

12.   (Currently amended) The method of ~~Claim~~claim 10, wherein ~~determining further~~ requesting comprises ~~determining if the mobile application being dispatched is a sensitive application and~~ requesting authentication if a sensitive mobile application is being dispatched.

13.   (Currently amended) The method of ~~Claim~~claim 10, wherein ~~determining further~~ requesting comprises ~~determining if the mobile application being dispatched is a sensitive application and~~ requesting authentication if a mobile application is being dispatched from a vulnerable host.

14.   (Currently amended) The method of ~~Claim~~claim 10, ~~wherein determining~~ further ~~comprises~~ comprising authenticating the dispatching host based on one or more rules defined by ~~an operator of the method~~ a user.

15.   (Currently amended) The method of ~~Claim 11~~claim 10, ~~wherein determining~~ further ~~comprises~~ comprising assigning a vulnerable classification or a non-vulnerable classification to each host ~~in the mobile application method~~.

16.   (Currently amended) The method of ~~Claim 11~~claim 10, ~~wherein determining~~ further ~~comprises~~ comprising assigning a sensitive classification or a non-sensitive classification to each mobile application ~~in the mobile application system~~ as the mobile application is created.

17.   (Currently amended) The method of ~~Claim~~claim 10, wherein each mobile application comprises an itinerary listing a node for each host to which the mobile application ~~jumps in the mobile application system~~, wherein each node indicates if authentication is required

to jump from the particular host and wherein ~~the determining~~ requesting further comprises requesting authentication based on the node in the itinerary.

18.   (Currently amended) The method of ~~Claim 11~~claim 10, wherein ~~the host~~ a host comprises one or more wireless ~~device~~ devices that are classified as vulnerable.

19.   (Currently amended) A mobile application security system, comprising:
    ~~one or more nodes of a peer-to-peer network wherein each node is configured to execute a mobile application;~~
    a management and security node connected to <u>one or more nodes of a peer-to-peer network, each node configured to execute a mobile application, the management and security node</u> ~~each node of the peer-to-peer network for controlling the security of a mobile application; the management and security node further~~ comprising means for monitoring ~~the~~ security of the mobile application as it jumps between the <u>one or more</u> nodes wherein data about the mobile application is communicated to the management and security node prior to the mobile application being dispatched from a dispatching node[[;]], ~~and wherein~~ the security monitoring means further ~~comprises~~ comprising means for determining if authentication of the dispatching node is required prior to dispatch of the mobile application <u>responsive to determining if the mobile application is a sensitive application and determining if the dispatching node is a vulnerable node, and means for requesting authentication if authentication of the dispatching host is required</u>.

20.   (Cancelled)

21.   (Currently amended) The system of ~~Claim~~claim 19, wherein the ~~determining~~ <u>requesting</u> means ~~further comprises means for determining if the mobile application being dispatched is a sensitive application and means for requesting~~ <u>requests</u> authentication if a sensitive mobile application is being dispatched.

22.   (Currently amended) The system of ~~Claim~~claim 19, wherein the ~~determining~~ <u>requesting</u> means ~~further comprises means for determining if the mobile application being~~

dispatched is a sensitive application and means for requesting requests authentication if a mobile
application is being dispatched from a vulnerable node.

23.   (Currently amended) The system of Claimclaim 19, wherein the determining
means management and security node further comprises means for authenticating the dispatching
node based on one or more rules defined by an operator of the system a user.

24.   (Currently amended) The system of Claim 20claim 19, wherein the determining
means management and security node further comprises means for assigning a vulnerable
classification or a non-vulnerable classification to each node in the mobile application system.

25.   (Currently amended) The system of Claim 20claim 19, wherein the determining
means management and security node further comprises means for assigning a sensitive
classification or a non-sensitive classification to each mobile application in the mobile
application system as the mobile application is created.

26.   (Currently amended) The system of Claimclaim 19, wherein each mobile
application comprises an itinerary listing a node for each node to which the mobile application
jumps in the mobile application system wherein each node indicates if authentication is required
to jump from the particular node and wherein the determining means further comprises means
for requesting means requests authentication based on the node in the itinerary.

27.   (Currently amended) The system of Claim 20claim 19, wherein the host a node
comprises one or more wireless device devices that are classified as vulnerable.

28.   (Currently amended) A mobile application security method, comprising:
        receiving data about a mobile application at a management and security node each time
the mobile application is being dispatched from a dispatching node in a peer-to-peer network;
and
        monitoring the security of the mobile application as it jumps between the nodes, wherein
the security monitoring further comprises determining if authentication of the dispatching node is

required prior to dispatch of the mobile application, including determining if the mobile application is a sensitive application and determining if the dispatching node is a vulnerable node; and

> requesting authentication if authentication of the dispatching node is required.

29.   (Cancelled)

30.   (Currently amended) The method of ~~Claim~~claim 28, wherein ~~the determining further~~ requesting comprises ~~determining if the mobile application being dispatched is a sensitive application and~~ requesting authentication if a sensitive mobile application is being dispatched.

31.   (Currently amended) The method of ~~Claim~~claim 28, wherein ~~the determining further~~ requesting comprises ~~determining if the mobile application being dispatched is a sensitive application and~~ requesting authentication if a mobile application is being dispatched from a vulnerable node.

32.   (Currently amended) The method of ~~Claim~~claim 28, ~~wherein the determining~~ further ~~comprises~~ comprising authenticating the dispatching node based on one or more rules defined by ~~an operator of the system~~ a user.

33.   (Currently amended) The method of ~~Claim~~claim 28, ~~wherein the determining~~ further ~~comprises~~ comprising assigning a vulnerable classification or a non-vulnerable classification to each node ~~in the mobile application system~~.

34.   (Currently amended) The method of ~~Claim~~claim 28, ~~wherein the determining~~ further ~~comprises~~ comprising assigning a sensitive classification or a non-sensitive classification to each mobile application ~~in the mobile application system~~ as the mobile application is created.

35.   (Currently amended) The method of ~~Claim~~claim 28, wherein each mobile application comprises an itinerary listing a node for each node to which the mobile application jumps ~~in the mobile application system~~ wherein each node indicates if authentication is required

Applicant : Christopher A. Rygaard   Attorney's Docket No.: 18511-008001
Serial N . : 09/851,763
Filed   : May 8, 2001
Page   : 9 of 15

to jump from the particular node and wherein ~~the determining~~ requesting further comprises requesting authentication based on the node in the itinerary.

36.   (Currently amended) The method of ~~Claim 29~~claim 28, wherein ~~the host~~ a node comprises one or more wireless ~~device~~ devices that are classified as vulnerable.

37.   (New) A mobile application security system, comprising:
a mobile application capable of jumping between hosts during execution; and
a management and security node, in communication with the hosts, the management and security node configured to determine whether to authenticate the mobile application while jumping between hosts responsive to a vulnerability classification of a dispatching host and a sensitivity classification of the mobile application, and request authentication if authentication of the dispatching host is required.

38.   (New) The mobile application security system of claim 37, wherein the management and security node requests authentication of the mobile application responsive to the dispatching host being classified as vulnerable and the mobile application being classified as sensitive.

39.   (New) The mobile application system of claim 38, wherein the dispatching host is classified as vulnerable if comprising one from the group containing a wireless device, a mobile device, a handheld device, and a laptop computer.

40.   (New) The mobile application security system of claim 37, wherein the management and security node does not request authentication of the mobile application responsive to the dispatching host being classified as non-vulnerable or the mobile application being classified as non-sensitive.

41.   (New) The mobile application system of claim 37, wherein the management and security node receives the mobile application from the dispatching host, and dispatches the

mobile application to the receiving host responsive to determining that no authentication is required or authenticating the mobile application.

42.   (New) The mobile application security system of claim 37, wherein the management and security node authenticates the mobile application including receiving a first authentication data prior a jump, receiving a second authentication data during the jump, and comparing the first and second authentication data.

43.   (New) The mobile application security system of claim 37, wherein the management and security node authenticates a user of the host.

44.   (New) The mobile application security system of claim 37, wherein the management and security node authenticates the dispatching host prior to dispatch.

45.   (New) The mobile application security system of claim 37, wherein the hosts do not include the management and security node.

46.   (New) The mobile application security system of claim 37, wherein the management and security node further comprises a host.

47.   (New) A mobile application security system, comprising:
a mobile application capable of jumping between hosts during execution; and
a dispatching host, in communication with a management and security node, the dispatching host configured to provide a vulnerability classification of the dispatching host and a sensitivity classification of the mobile application to the management and security node prior to dispatch, and to assist authentication of a user of the dispatching host responsive to receiving an authentication request.

48.   (New) The mobile application security system of claim 47, wherein the dispatching host sends authentication information to the management and security node to perform authentication.

49.   (New) The mobile application security system of claim 47, wherein the dispatching host dispatches the mobile application to the management and security node.